all involved with the daily management of the agency's information resources, including the accuracy, availability, and safety of these resources. Each agency assigns responsibility somewhat differently, but as a group these persons issue procedures, guidelines, and standards to implement the agency's policy for information security, and to monitor its effectiveness and efficiency. They provide technical assistance to users, functional managers, and to the data processing organization in such areas as risk assessment and available security products and technologies. They review and evaluate the functional and program groups' performance in information security.

(4) *Automated Data Processing (ADP) Management, Operations, and Programming Staff* are all involved with the daily management and operations of the automated data processing services. They provide for the protection of the data in their custody and identify to the data owners what those security measures are. This group includes such diverse positions as computer operators, schedulers, tape librarians, data base administrators, and systems and applications programmers. They provide the technical expertise for implementing security-related controls within the automated environment. They have primary responsibility for all aspects of contingency planning.

(5) *End Users* are any employees who have access to an agency computer system that processes sensitive information. This is the largest and most heterogenous group of employees. It consists of everyone from the executive who has a personal computer with sensitive information to data entry clerks.

(c) The training guidelines developed by the National Institute of Standards and Technology identify five subject areas. They are:

(1) *Computer security basics* is the introduction to the basic concepts behind computer security practices and the importance of the need to protect the information from vulnerabilities to known threats;

(2) *Security planning and management* is concerned with risk analysis, the determination of security requirements, security training, and internal agency organization to carry out the computer security function;

(3) *Computer security policies and procedures* looks at Governmentwide and agency-specific security practices in the areas of physical, personnel software, communications, data, and administrative security;

(4) *Contingency planning* covers the concepts of all aspects of contingency planning, including emergency response plans, backup plans and recovery plans. It identifies the roles and responsibilities of all the players involved; and

(5) *Systems life cycle management* discusses how security is addressed during each phase of a system's life cycle (e.g. system design, development, test and evaluation, implementation, and maintenance). It addresses procurement, certification, and accreditation.

(d) The statute defines the term *sensitive information* as any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

§930.302 Training requirement.

The head of each agency shall identify employees responsible for the management or use of computer systems that process sensitive information and provide the following training (consult ''Computer Security Training Guidelines,'' NIST Special Publication 500–172[1], for more detailed information) to each of these groups:

(a) Executives shall receive awareness training in computer security basics, computer security policy and procedures, contingency planning, and systems life cycle management; and policy level training in security planning and management.

[1] Copies may be ordered from the Superintendent of Documents, U.S. Government Printing Office, Washington, DC 20402–9325.

(b) Program and functional managers shall receive awareness training in computer security basics; implementation level training in security planning and management, and computer security policy and procedures; and performance level training in contingency planning and systems life cycle management.

(c) IRM, security, and audit personnel shall receive awareness training in computer security basics; and performance level training in security planning and management, computer security policies and procedures, contingency planning, and systems life cycle management.

(d) ADP management and operations personnel shall receive awareness training in computer security basics; and performance level training in security planning and management, computer security policies and procedures, contingency planning, and systems life cycle management.

(e) End users shall receive awareness training in computer security basics, security planning and management, and systems life cycle management; and performance level training in computer security policies and procedures, and contingency planning.

§ 930.303 Initial training.

The head of each agency shall provide the training outlined in § 930.302 of this subpart to all such new employees within 60 days of their appointment.

§ 930.304 Continuing training.

The head of each agency shall provide training whenever there is a significant change in the agency information security environment or procedures or when an employee enters a new position which deals with sensitive information.

§ 930.305 Refresher training.

Computer security refresher training shall be given as frequently as determined necessary by the agency based on the sensitivity of the information that the employee uses or processes.

PART 950—SOLICITATION OF FEDERAL CIVILIAN AND UNIFORMED SERVICE PERSONNEL FOR CONTRIBUTIONS TO PRIVATE VOLUNTARY ORGANIZATIONS

Subpart A—General Provisions

Subpart B—Eligibility Provisions

Subpart C—Federations

Subpart D—Campaign Materials

Subpart E—Undesignated Funds

Subpart F—Miscellaneous Provisions

Subpart G—DoD Overseas Campaign

Subpart H—CFC Timbetable